



EUROPEAN COMMISSION
Information Society and Media Directorate-General
Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 25 March 2009

WORKSHOP ON THE EU POLICY DIMENSION OF VULNERABILITY MANAGEMENT AND DISCLOSURE PROCESS

31 March 2009, 09.30-16.30

BU25 0/S1

25, avenue de Beaulieu - 1160 Brussels

Contact: Valérie ANDRIANAVALY, DG Information Society & Media - INFSO
Tel +32 2 299 62 02, valerie.andrianavaly@ec.europa.eu

1. INTRODUCTION

In July 2008, a vulnerability note¹ released by the United States Computer Emergency Readiness Team (US-CERT) revealed deficiencies in the DNS protocol and common DNS implementations that facilitate DNS cache poisoning attacks². In October 2008, the Finnish Computer Emergency Response Team (CERT-FI) released a statement³ that they are co-ordinating the work, with relevant vendors and its discoverers, regarding a vulnerability in the TCP protocol⁴.

In both cases, the discovered vulnerabilities affect widespread protocols providing basic infrastructural services on the Internet and had the potential to impact a large number of vendors and users. Moreover, in both cases, the full details of the attack have not been disclosed for a certain period to give enough time to researchers and vendors to find a solution. Specific CERTs have been coordinating work into the security issue and providing detailed information to software vendors affected.

¹ See <http://www.kb.cert.org/vuls/id/800113>

² The vulnerability allows an external attacker, under certain conditions, to alter the information returned by "DNS servers" in response to a request of translation of a domain name like ec.europa.eu into the IP address of the equipment hosting the related web page. This could entail that a user could be directed to a web site which is not the legitimate one. The fake website, using similar graphics and text, could pretend to be the legitimate one and thus mislead the user. The discovery was credited to security researcher Dan Kaminsky. See some details of the process of handling the vulnerability at http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky?currentPage=all.

³ See <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

⁴ According to publicly available data, the vulnerability is based on a denial of service on the TCP connection queue of a target host. The vulnerability can be exploited with relatively small amounts of traffic. CERT-FI statement mentions that work on determining the scope and impact of the vulnerability is currently ongoing, and will be followed by a coordinated process of patching and publication. Additional details about the issue will be published following the guidelines of responsible disclosure.

2. POLICY CONTEXT

In March 2009, the European Commission intends to launch a policy initiative on Critical Information Infrastructure Protection (CIIP)⁵. This initiative will constitute a significant step forward in the implementation of the Commission's strategy for a Secure Information Society⁶ adopted in 2006. The planned activities will be conducted under and in parallel to the broader framework of the European Programme on Critical Infrastructure Protection⁷.

The aim of this initiative is to enhance the protection of Europe from large scale cyber-attacks and disruptions by enhancing preparedness, security and resilience of Critical Information Infrastructures (CII). It focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs. Relevant public and private stakeholders will be engaged in ensuring that adequate and consistent levels of preventive, detection, emergency and recovery measures are put in operation to ensure the appropriate levels of security and resilience of CIIs and guarantee the continuity of services.

One of the actions envisaged is the creation of a strong and trusted European Public Private Partnership (PPP) for resilience of CIIs that would support the exchange of information and knowledge on specific topics with an EU and international dimension. The present workshop is organised in that context.

3. OBJECTIVES OF THE WORKSHOP

The objectives of the workshop are to i) exchange between participants experiences regarding current vulnerability management and disclosure approaches and discuss lessons learnt; ii) discuss the need and merits to promote vulnerability management activities throughout the EU; iii) identify priority areas and possible mechanisms for policy actions to enhance the preparedness in handling and coordinating vulnerability management and disclosure at the EU level and in cooperation with international partners.

4. SCOPE OF THE WORKSHOP

The aim is to explore the policy dimension of vulnerability management, in particular the aspects of risks assessment and responsible vulnerability disclosure. To this end, the experiences gained from existing practices and schemes will be discussed with a view to identify the needs and the scope for action at the EU.

The debate would address relevant aspects of vulnerability management and disclosure among which could be the following questions:

- (1) **Risk assessment:** When a vulnerability which could potentially affect a large number of products and users is discovered, the global risks to the society and economy need to be assessed. In that respect, the following questions could be raised:

⁵ See COM(2007)640 of 23.10.2007 regarding Commission Legislative & Work Programme for 2008

⁶ See COM(2006)251 of 31.05.2006.

⁷ See COM(2006)786 of 12.12.2006

- (a) What are the role of governments, CERTs, vendors, researchers, corporate users and individuals in terms of assessing the global risk for the society and the economy? Who are the precise stakeholders to be involved? What role should have each of them?
 - (b) What are the information exchange schemes that are in place between security experts / technology vendors and EU governments on vulnerabilities and threats (in particular regarding the Internet)? What are the needs they address? Is there any need for more national as well as trans-national cooperation (at national, EU or international levels) on risk assessment once a specific vulnerability is discovered?
- (2) **The coordination of vulnerability disclosures:** Recent events have witnessed a process of managing large scale vulnerabilities in which the initial steps (discovery and search for a solution) are handled among a circle of trusted partners. In this kind of context, policy makers might be called to reflect on the need to ensure that all EU stakeholders are put on an equal footing and that they are not put at a disadvantage in cases where the discovery of a vulnerability is made in a third country.
- (a) Who are the stakeholders to be involved in the vulnerability disclosure? What role should have each of them?
 - (b) What should be the constituent elements of a possible framework to ensure trust and support the cooperation between stakeholders?
 - (c) Is there any need for more national as well as trans-national cooperation (at national, EU or international levels) on vulnerability disclosure? If relevant, what could be the mechanisms to support national and trans-national cooperation? Could voluntary principles to guide the disclosure of potentially valuable information to third parties be a suitable mechanism to engage relevant stakeholders (governments, researchers, CERTs and vendors)? *One dilemma to be considered is the extent to which openness and transparency could be ensured so that all the interested stakeholders are promptly and fully informed of relevant technical details of any security threat while at the same time avoiding leakage to the "bad guys".*
 - (d) What should be the policy principles to enhance the conditions for supporting the establishment of the trust needed to exchange the details of vulnerabilities? What should possibly be changed and/or adapted when moving from a national to a trans-national EU level? *This might call reflections on the best way to ensure that the ones outside the "trusted circle" are not put at a commercial or political disadvantage.*
- (3) **Deployment of solutions:** The deployment of solutions at a large scale might be quite challenging. A recent DNS survey found that, still, *"nearly one in four DNS servers remain un-upgraded—and vulnerable to cache poisoning"*⁸;

⁸ See <http://www.infoblox.com/library/pdf/2008-survey-executive-summary.pdf>. The report further notes that the effort by vendors and the Internet's DNS community to encourage administrators to upgrade their name servers after the announcement of the

- (a) Which measures and/or mechanisms could be envisaged at national and EU level to support the smooth deployment of solutions especially when vulnerabilities with large scale impacts need to be fixed? Which communities (like the entities with National Incident Response Capability or CERTs) should be engaged?

These points should be considered as a guideline for the discussion and not as a constraint. Participants are welcomed to address any other relevant dimensions in the scope of the workshop (i.e. policy or enhanced cooperation related).

5. FORMAT OF THE WORKSHOP AND DATE

The workshop is planned for the 31st of March 2008 in Brussels and is based on presentations to set the scene, present experiences and lessons learnt, provide view points and foster the discussions on the desirability and way forward of an EU action plan for enhancing vulnerability management.

6. PROFILE OF PARTICIPANTS

The workshop is open to Member State officials and experts involved in policy making in Network and Information Security and Critical Information Infrastructure Protection. Experts from the Internet and CERT communities as well as from the NIS and ICT industry will be invited.

7. PRACTICAL ORGANISATION

N.B. Due to budgetary constraints, the Commission will not be able to reimburse any travel expenses.

Kaminsky vulnerability paid off; however, a surprising number have not been upgraded and are very vulnerable to cache poisoning.

8. AGENDA

9 h 00 *Registration & Coffee*

09 h 30 **Setting the scene**

09 h 30 Introduction to the workshop

09 h 40 Update on the CIIP initiative - Andrea Glorioso

10 h 00 State of play on vulnerability disclosure - Prof. Juha Rönning

10 h 20 **Exchange of experiences and lessons learnt**

10 h 20 Erka Koivunen - CERT-FI

10 h 40 Andy Schunmann - CPNI-UK

11 h 00 *Coffee break*

11 h 30 Stanislas de Maupeou - CERTA-FR

11 h 50 Konstantin Knorr - CT IC CERT SIEMENS

12 h 10 Camillo Särs - F-SECURE

12 h 30 *Lunch break*

14 h 00 Damir Rajnovic - CISCO - ISO draft standard on responsible vulnerability disclosure - ISO/IEC 29147 (video link)

14 h 20 **Open discussion on vulnerability management and disclosure in the EU**

14 h 20 Tour de table and debate

The debate will be steered by the questions identified in the description of the workshop (chapter 4 above) and will cover the following areas:

- *Risk assessment*
- *Coordination of vulnerability disclosures*
- *Deployment of solutions*

15 h 45 *Coffee break*

16 h 00 **The way forward**

16 h 00 Tour de table on conclusions, key priorities and means for actions at the EU level

16 h 30 End of the workshop

./.